Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

99890248.0

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE

20/01/00

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 99890248.0

Anmeldetag:
Date of filing:
Date de dépôt: 22/07/99

Anmelder:
Applicant(s):
Demandeur(s):
Koninklijke Philips Electronics N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Datenträger zum Speichern von Daten und Schaltung für einen solchen Datenträger

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Datenträger zum Speichern von Daten und Schaltung für einen solchen Datenträger

Die Erfindung bezieht sich auf einen Datenträger gemäß dem Oberbegriff des Anspruches 1.

Die Erfindung bezieht sich weiters auf eine elektrische Schaltung gemäß dem Oberbegriff des Anspruches 7.

Die Erfindung bezieht sich weiters auf ein Verfahren gemäß dem Oberbegriff des Anspruches 13.

Ein solcher Datenträger und eine solche Schaltung und ein solches Verfahren sind aus dem Dokument WO 97/29454 bekannt. Der bekannte Datenträger ist durch eine sogenannte Smart-Card gebildet.

Bei dem bekannten Datenträger ist ein kontaktloses erstes Interface zum kontaktlosen Kommunizieren mit einer Kommunikationseinrichtung vorgesehen. Bei einer kontaktlosen Kommunikation ist mit Hilfe einer induktiven Kopplung zwischen einer Übertragungsspule der Kommunikationseinrichtung und einer Übertragungsspule des kontaktlosen Interfaces mit Hilfe eines hochfrequenten Trägersignals sowohl eine Übertragung von Energie zum Datenträger zwecks Erzeugung einer Versorgungsspannung für die Schaltung des Datenträgers als auch ein Austausch von Daten zwischen dem Datenträger und der Kommunikationseinrichtung realisiert.

Der bekannte Datenträger weist weiters ein kontaktbehaftetes zweites Interface zum kontaktbehafteten Kommunizieren mit einer Kommunikationseinrichtung auf. Das kontaktbehaftete Interface ist gemäß dem Standard ISO 7816 ausgebildet, womit eine Zuführung einer Versorgungsspannung für die Schaltung und ein Austausch von Daten über die Kontakte von diesem Interface ermöglicht ist.

Der bekannte Datenträger verfügt über Speichermittel zum Speichern von Daten in mehreren Speicherbereichen, wobei die Speichermittel als Halbleiterspeicher vom Typ EEPROM ausgebildet sind.

Auf einen ersten Speicherbereich ist von einem ersten Speicherzugriffsmittel her zugreifbar, wobei das erste Speicherzugriffsmittel durch ein erstes Betriebssystem gebildet

ist, das unter der Marke „Mifare" bekannt geworden ist. Dieses erste Betriebssystem unterstützt ein erstes Kommunikationsprotokoll, so daß bei einer Kommunikation über das kontaktlose Interface und bei einem Zugreifen auf den ersten Speicherbereich ein authentisierter Zugriff des ersten Betriebssystems gemäß dem Standard ISO/IEC DIS9798-2 auf den ersten Speicherbereich gewährleistet ist. Ein wesentlicher Bestandteil dieser Authentisierung ist die Geheimhaltung von in dem ersten Speicherbereich gespeicherten Schlüsseln.

Auf den zweiten Speicherbereich ist von einem zweiten Betriebssystem, nämlich einem User-Betriebssystem her über ein zweites Speicherzugriffsmittel zugreifbar, wobei das zweite Speicherzugriffsmittel durch Teile des ersten Betriebssystems gebildet ist. Das zweite Betriebsystem kann ein beliebiges zweites Kommunikationsprotokoll unterstützen.

Bei dem bekannten Datenträger sind weiters Zugriffsermöglichungsmittel vorgesehen, mit denen sichergestellt ist, daß bei einer Kommunikation über das kontaktlose Interface alleinig von dem ersten Betriebssystem her auf den ersten Speicherbereich zugreifbar ist und daß bei einer Kommunikation über das kontaktbehaftete Interface alleinig von dem zweiten Betriebssystem her auf den zweiten Speicherbereich zugreifbar ist. Die Zugriffsermöglichungsmittel sind bei einem Zusammenwirken des jeweils zugreifenden Speicherzugriffsmittels mit einer Zugriffsermöglichungsstufe realisiert. Die Zugriffsermöglichungsstufe ist unveränderlich in einem ROM gespeichert und ermöglicht oder verweigert über in sie eingetragene Zugriffsermöglichungen das Zugreifen der Speicherzugriffsmittel auf die verschiedenen Speicherbereiche.

Bei dem bekannten Datenträger ist also durch das Vorsehen des ersten Kommunikationsprotokolls ein variabler erster Schutz und durch das Vorsehen der Zugriffsermöglichungsmittel ein unveränderlicher zweiter Schutz, also zusammen ein doppelter Schutz vor unbefugten Zugriffen auf die Daten in dem ersten Speicherbereich gegeben.

In der Praxis wird der bekannte Datenträger häufig bei zwei unterschiedlichen Systembetreibern eingesetzt. Der erste Systembetreiber kann beispielsweise ein Beförderungsunternehmen sein, das bei einer Kommunikation über das kontaktlose Interface mit Hilfe des ersten Betriebssystems auf in dem ersten Speicherbereich gespeicherte Daten, die beispielsweise Beförderungseinheiten repräsentieren, zugreifen muß. Der zweite Systembetreiber kann ein Bankunternehmen sein, das bei einer Kommunikation über das kontaktbehaftete Interface mit Hilfe des zweiten Betriebssystems, welches auf Grund von komplexen Anforderungen des

Bankunternehmens meist unabhängig von dem ersten Betriebssystem implementiert wird, auf in dem zweiten Speicherbereich gespeicherte Daten, die beispielsweise Geldbeträge repräsentieren, zugreifen muß. Es ist also bei einer derartigen Konfiguration verständlich, daß beide Systembetreiber im eigenen Sinne und im Sinne Ihrer Kunden einen größtmöglichen Schutz der in den jeweiligen Speicherbereichen gespeicherten Daten gegenüber unbefugten Zugriffen durch das Betriebssystem des anderen Systembetreibers fordern und daß dieser Forderung durch das Zugriffszuordnungsmittel vollends Rechnung getragen wird.

Im Falle einer Kooperation der Systembetreiber kann es aber erwünscht sein, daß gemäß dem vorstehend erwähnten Beispiel das Bankunternehmen zum Zweck der direkten Verrechnung von Dienstleistungen des Beförderungsunternehmens auf dessen auf dem Datenträger im ersten Speicherbereich gespeicherte Daten (z.B. Daten über Beförderungseinheiten) zugreifen soll. Dies kann konkret bedeuten, daß bei einer Kommunikationseinrichtung (Bankterminal) des Bankunternehmens Beförderungseinheiten repräsentierende Daten in den Speicherbereich des Beförderungsunternehmens, also in den ersten Speicherbereich, aufbuchbar sein sollen.

Bei dem bekannten Datenträger bestünde eine erste Möglichkeit eine Kooperation zwischen den Systembetreibern zu erlauben, indem mit einer Erweiterung des ersten Kommunikationsprotokolls bei einer Kommunikation über das kontaktbehaftete Interface dem zweiten Betriebssystem das Recht zugewiesen wird, über das erste Betriebssystem gemäß dem ersten Kommunikationsprotokoll und bei Kenntnis der zur Authentisierung notwendigen Schlüssel auf den ersten Speicherbereich zuzugreifen.

Von dieser Möglichkeit wird aber kein Gebrauch gemacht. Es müßten nämlich der von dem Bankunternehmen zur Kommunikation mit dem Datenträger eingesetzten Kommunikationseinrichtung die in dem ersten Speicherbereich, also in dem Speicherbereich des Beförderungsunternehmens gespeicherten Schlüssel bekannt sein. Damit wäre zwar die Authentisierung durchführbar, zugleich würde aber der wesentliche Bestandteil der Authentisierung, nämlich die Geheinhaltung der Schlüssel, verletzt. Somit wäre der erste Schutz äußerst nachteilig aufgeweicht.

Bei dem bekannten Datenträger bestünde weiters eine zweite Möglichkeit einer Kooperation zwischen den Systembetreibern, bei der die Authentisierung mit Hilfe der Schlüssel gemäß dem ersten Kommunikationsprotokoll entfällt. Hierbei würde jedoch der von dem Beförderungsunternehmen geforderte erste Schutz vor unbefugten Zugriffen auf die Daten in dem ersten Speicherbereich völlig ausgeschaltet.

Die Erfindung hat sich zur Aufgabe gestellt, die bei einem Datenträger entsprechend der im Oberbegriff des Anspruches 1 angeführten Gattung und die bei einer elektrischen Schaltung entsprechend der im Oberbegriff des Anspruch 7 angeführten Gattung und die bei einem Verfahren entsprechend der im Oberbegriff des Anspruches 13 angeführten Gattung auftretenden Schwierigkeiten zu vermeiden und einen verbesserten Datenträger, eine verbesserte Schaltung und ein verbessertes Verfahren zu realisieren, so daß eine Kooperation von zwei Systembetreibern bei gleichbleibendem hohem Schutz der in dem ersten Speicherbereich gespeicherten Daten gegenüber unbefugten Zugriffen ermöglicht ist.

Zur Lösung der vorstehend angeführten Aufgabe sind bei einem Datenträger gemäß der im Oberbegriff des Anspruches 1 angegebenen Gattung gemäß der Erfindung die Merkmale gemäß dem kennzeichnenden Teil des Anspruches 1 vorgesehen.

Zur Lösung der vorstehend angeführten Aufgabe sind weiters bei einer Schaltung gemäß der im Oberbegriff des Anspruches 7 angeführten Gattung gemäß der Erfindung die Merkmale gemäß dem kennzeichnenden Teil des Anspruches 7 vorgesehen.

Zur Lösung der vorstehend angeführten Aufgabe sind weiters bei einem Verfahren gemäß der im Oberbegriff des Anspruches 13 angegebenen Gattung gemäß der Erfindung die Merkmale gemäß dem kennzeichnenden Teil des Anspruches 13 vorgesehen.

Durch das Vorsehen der erfindungsgemäßen Merkmale gemäß den Ansprüchen 1, 7 und 13 ist auf äußerst vorteilhafte Weise erreicht, daß nach dem Prüfen einer Zugriffsberechtigung und dem Erhalt eines positiven Ergebnisses der Prüfung dieser Zugriffsberechtigung von dem zweiten Speicherzugriffsmittel her über nicht in den zweiten Speicherzugriffsmitteln vorgesehene Speicherzusatzzugriffsmittel und über die ersten Speicherzugriffsmittel auf den ersten Speicherbereich zugreifbar ist.

Damit ist durch das Vorsehen der Speicherzusatzzugriffsmittel in dem Datenträger bzw. in der Schaltung der Vorteil erhalten , daß eine Kooperation von zwei Systembetreibern auf einfache Weise ermöglichbar ist, wobei aber für beide Systembetreiber eine hohe Sicherheit gegenüber unbefugten Zugriffen auf ihre Speicherbereiche gewährleistet bleibt.

Ein zweiter Vorteil ist dadurch erhalten, daß eine durch die Zugriffsermöglichungsmittel realisierte Unterbindung eines direkten Zugriffes von dem zweiten Speicherzugriffsmittel auf den ersten Speicherbereich aufrecht erhalten ist und zugleich ein Zugreifen von dem zweiten Speicherzugriffsmittel über das erste

Speicherzugriffsmittel auf den ersten Speicherbereich nach einem Prüfen von Zugriffsberechtigungen zum Schutz vor unbefugten Zugriffen auf den ersten Speicherbereich ermöglicht ist.

Als dritter Vorteil ergibt sich durch das Zugreifen von den zweiten Speicherzugriffsmitteln mit Hilfe der ersten Speicherzugriffsmittel auf die in dem ersten Speicherbereich gespeicherten Daten, daß für eine einwandfreie Konsistenz des Zugreifens gesorgt ist. Dadurch ist eine Verfügbarkeit dieser Daten bei einer Kommunikation basierend auf einem Kommunikationsprotokoll der ersten Speicherzugriffsmittel sichergestellt.

Als vierter Vorteil ist eine individuelle Gestaltung der Zugriffsberechtigungen ebenso wie eine flexible Verwaltung dieser Zugriffsberechtigungen während der Lebenszeit eines erfindungsgemäßen Datenträgers gewährleistet, da von einem Systembetreiber, beispielsweise von einem Beförderungsunternehmen, bei einer Kommunikation zwischen dem Datenträger und der kontaktlosen Kommunikationseinrichtung problemlos Zugriffsberechtigungen erteilt, verweigert und modifiziert werden können.

Das Vorsehen des erfindungsgemäßen Merkmals gemäß den Ansprüchen 2 und 8 ermöglicht auf vorteilhafte Weise eine Nutzung von bereits in dem ersten Speicherzugriffsmittel vorhandenen Softwareroutinen, wodurch sich die erfindungsgemäßen Merkmale auf besonders einfache Weise realisieren lassen.

Durch das Vorsehen der erfindungsgemäßen Merkmale gemäß den Ansprüchen 3, 9 und 14 ergeben sich die folgenden Vorteile. Es ist erstens der Vorteil gegeben, daß bei einer Prüfung von einem Zugriffcode mit Hilfe der Zugriffcodeprüfmittel ein aus den Daten des ersten Speicherbereiches berechenbarer Zugriffscode verwendet wird. Dies hat sich besonders in bezug auf eine Geheimhaltung von in dem ersten Speicherbereich gespeicherten Schlüsseln als vorteilhaft ergeben, weil nicht ein Schlüssel selbst zum Prüfen herangezogen wird, sondern ein aus ihm berechenbarer Zugriffscode. Zweitens ist auch die Verwendung eines von dem zweiten Speicherzugriffsmittel her zuführbaren Zugriffscode bei der Prüfung der Zugriffsberechtigung äußerst vorteilhaft, weil damit eine größtmögliche Flexibilität bezüglich des Ursprunges dieses zuführbaren Zugriffscodes gegeben ist. So kann ein zuführbarer Zugriffscode beispielsweise in den Daten des zweiten Speicherbereiches gespeichert oder ebenfalls aus diesen Daten berechenbar sein. Als besonders vorteilhaft hat es sich in diesem Zusammenhang erwiesen, wenn ein zuführbarer Zugriffscode bei einer Kommunikation zwischen dem Datenträger und einer Kommunikationseinrichtung über eines der beiden Interface verschlüsselt kommuniziert

wird.

Bei einem erfindungsgemäßen Datenträger und einer erfindungsgemäßen Schaltung hat sich das Vorsehen der erfindungsgemäßen Merkmale gemäß dem Anspruch 4 und dem Anspruch 10 in zweierlei Hinsicht als äußerst vorteilhaft erwiesen. Erstens wird durch das Vorsehen eines speziell zur Berechnung eines berechenbaren Zugriffscodes vorgesehenen Zugriffscodeberechnungsmittels die Abarbeitung der Berechnung beschleunigt, wodurch eine wesentlich verkürzte Dauer der Kommunikation zwischen dem Datenträger und einer Kommunikationseinrichtung ermöglicht ist. Zweitens verhindert die Abarbeitung eines Triple DES Verschlüsselungsverfahrens gemäß dem Standard ISO/IEC 10116, daß ein dem berechenbaren Zugriffscode zugrunde liegender Schlüssel aus dem Zugriffscode durch eine Anwendung eines inversen Verschlüsselungsverfahrens auf einen aus diesem Schlüssel berechneten Zugriffscode berechnet werden kann.

Das Vorsehen der erfindungsgemäßen Merkmale gemäß den Ansprüchen 5, 11 und 15 hat sich zusätzlich als äußerst vorteilhaft erwiesen. Hierdurch ist nämlich erreicht, daß zum Schutz gegenüber unbefugten Zugriffen auf den ersten Speicherbereich bei der Prüfung von Zugriffsberechtigungen zusätzlich zu der Prüfung von Zugriffscodes eine Prüfung von Zugriffsbedingungen (Schreiben, Lesen) vorgesehen ist. Hierdurch ist auf einfache Weise sichergestellt, daß selbst bei einem Übereinstimmen eines zuführbaren Zugriffscodes mit einem berechenbaren Zugriffscode eine zusätzliche Prüfung erfolgt, bevor endgültig bei einer zusätzlichen Übereinstimmung dieser Zugriffsbedingungen ein positives Ergebnis der Prüfung der Zugriffsberechtigung vorliegt. Durch diese Maßnahme ist eine hierarchische Gestaltung der Vergabe der Zugriffsberechtigung vorsehbar, wodurch auf einfache Weise ein größtmöglicher Schutz gegenüber unbefugten Zugriffen auf den ersten Speicherbereich sichergestellt ist.

Bei einem erfindungsgemäßen Datenträger und einer erfindungsgemäßen Schaltung hat sich das Vorsehen der erfindungsgemäßen Merkmale gemäß den Ansprüchen 6 und 12 als vorteilhaft erwiesen, weil dadurch eine möglichst kostengünstige Herstellung bei entsprechend hohen Stückzahlen gewährleistet ist.

Die vorstehend angeführten Aspekte und weitere Aspekte der Erfindung gehen aus dem nachfolgend beschriebenen Ausführungsbeispiel hervor und sind anhand dieses Ausführungsbeispieles erläutert.

Die Erfindung wird im Folgenden anhand von einem in den Zeichnungen dargestellten

Ausführungsbeispiel weiter beschrieben, auf das die Erfindung aber nicht beschränkt ist.

Die Figur 1 zeigt auf schematische Weise in Form eines Blockschaltbildes einen Datenträger, der Speicherzusatzzugriffsmittel aufweist.

Die Figur 2 zeigt in Form eines Flußdiagramms ein Verfahren zum Zugreifen auf Speichermittel des Datenträgers gemäß Figur 1.

Die Figur 1 zeigt in Form eines Blockschaltbilds einen Datenträger 1 zum Speichern von Daten, der eine Smart Card bildet und der zum Kommunizieren mit einer ersten Kommunikationseinrichtung 2 und einer zweiten Kommunikationseinrichtung 3 ausgebildet ist. Eine solche Smart Card ist durch eine Plastikkarte gebildet, die einen Halbleiterchip aufnimmt, der eine elektrische Schaltung bildet, und ist seit langem bekannt.

Die erste Kommunikationseinrichtung 2 ist zum kontaktlosen Kommunizieren mit dem Datenträger 1 ausgebildet und weist ein erstes Sende/Empfangsmittel 4 auf. Das erste Sende/Empfangsmittel 4 ist zum Modulieren eines Trägersignals gemäß einer Amplitudenmodulation mit ersten Sendedaten SD1 ausgebildet, die den ersten Sende/Empfangsmitteln 4 von einem in der Figur 1 nicht dargestellten ersten Kommunikationsmittel her zuführbar sind. Das amplitudenmodulierte Trägersignal wird einer Sende/Empfangsantennenkonfiguration 5 zugeführt und von dieser abgestrahlt. Andererseits sind über die Sende/Empfangsantennenkonfiguration 5 Unterschiede in der Belastung des abgestrahlten amplitudenmodulierten Trägersignals von dem ersten Sende/Empfangsmittel 4 als Belastungsmodulation detektierbar und nach einer Demodulation als erste Empfangsdaten ED1 an das erste Kommunikationsmittel abgebbar. Im vorliegenden Fall ist die Sende/Empfangsantennenkonfiguration 5 als Primärspule eines bei dem kontaktlosen Kommunizieren benötigten Kommunikationsspulenpaares 6 ausgebildet.

Die zweite Kommunikationseinrichtung 3 ist zum kontaktbehafteten Kommunizieren mit dem Datenträger 1 ausgebildet und weist ein zweites Sende/Empfangsmittel 7 auf. Das zweite Sende/Empfangsmittel 7 beinhaltet aus stiftartigen Kontakten bestehende Kontaktmittel 8 eines bei dem kontaktbehafteten Kommunizieren benötigten Kontaktepaares 9. Die Kontaktmittel 8 sind gemäß dem Standard ISO 7816 ausgebildet. Bei dem kontaktbehafteten Kommunizieren sind an ein in der Figur 1 nicht dargestelltes zweites Kommunikationsmittel einerseits zweite Empfangsdaten ED2 von dem zweiten

Sende/Empfangsmittel 7 abgebbar und andererseits sind dem zweiten Sende/Empfangsmittel 7 von dem zweiten Kommunikationsmittel her zweite Sendedaten SD2 zuführbar. Das zweite Sende/Empfangsmittel 7 weist weiters erste Pegelanpassungsmittel auf, welche zum Anpassen von Signalpegeln der zweiten Sendedaten SD2 und der zweiten Empfangsdaten ED2 vorgesehen sind.

Der Datenträger 1 weist ein kontaktloses erstes Interface 10 zum Kommunizieren mit der ersten Kommunikationseinrichtung 2 auf. Das erste Interface 10 beinhaltet eine Sekundärspule 11 des Kommunikationsspulenpaares 6, welche mit Schaltungsteilen des ersten Interfaces, nämlich mit einem in einer elektrischen Schaltung 12 des Datenträgers 1 enthaltenen ersten Versorgungsspannungsmittel 13 und mit einem in der elektrischen Schaltung 12 enthaltenen ersten Taktgenerator 14 und mit einem in der elektrischen Schaltung 12 enthaltenen ersten Signalkonvertierungsmittel 15 verbunden ist.

Bei einem Empfang eines Trägersignals mit der Sekundärspule 11 generiert das erste Versorgungsspannungsmittel 13 aus dem empfangenen Trägersignal eine erste Versorgungsspannung V1, die für eine elektrische Versorgung der elektrischen Schaltung 12 bei einer kontaktlosen Kommunikation vorgesehen ist. Bei einem Auftreten eines nominalen Wertes der ersten Versorgungsspannung V1 wird von dem ersten Versorgungsspannungsmittel 13 ein erstes Startsignal POR1 an ein erstes Betriebssystem 16 abgegeben.

Der erste Taktgenerator 14 erzeugt bei dem Empfang des Trägersignals einen ersten Systemtakt CLK1. Der erste Systemtakt CLK1 wird einerseits zum Zweck eines synchronen Kommunizierens zwischen der ersten Kommunikationseinrichtung 2 und dem ersten Interface 10 dem ersten Signalkonvertierungsmittel 15 zugeführt. Der erste Systemtakt CLK1 wird andererseits dem ersten Betriebssystem 16 als ein Betriebstakt zum Zweck eines synchronen Bearbeitens von zwischen dem Signalkonvertierungsmittel 15 und dem ersten Betriebssystem 16 bidirektional austauschbaren ersten Empfangsinformationen EI1 und ersten Sendeinformationen SI1 zugeführt.

Wenn der Datenträger 1 in die Nähe der ersten Kommunikationseinrichtung 2 gebracht wird und über das Kommunikationsspulenpaar 6 ein Trägersignal übertragen wird, dann befindet sich der Datenträger 1 innerhalb eines Kommunikationsbereiches der ersten Kommunikationseinrichtung 2. Bei einem in dem Kommunikationsbereich befindlichen Datenträger 1 wird zunächst durch den Empfang des Trägersignals, das gemäß dem vorliegenden Beispiel eine Frequenz von 13.56 MHz aufweist, die erste Versorgungsspannung V1 für die elektrische Schaltung 12 aufgebaut, danach wird der

Systemtakt CLK1 erzeugt und anschließend wird die Abarbeitung des ersten Betriebssystems 16 mit dem Startsignal POR1 gestartet. Mit Hilfe des ersten Betriebssystems 16 wird zunächst gemäß einem ersten Kommunikationsprotokoll eine Selektion eines einzigen Datenträgers 1 von möglicherweise mehreren innerhalb des Kommunikationsbereiches anwesenden Datenträgern 1 vollzogen, wonach mit einem selektierten Datenträger 1 eine Kommunikation aufgebaut werden kann. Eine solche Selektion ist im Zusammenhang mit der kontaktlosen Kommunikation seit langem bekannt.

Bei dem kontaktlosen Kommunizieren wird das empfangene Trägersignal einem in den ersten Signalkonvertierungsmitteln 15 enthaltenen Demodulator zugeführt, der zum Demodulieren des amplitudenmodulierten Trägersignals und zum Abgeben von ersten Empfangsinformationen EI1 an das erste Betriebssystem 16 ausgebildet ist. Bei dem kontaktlosen Kommunizieren werden erste Sendeinformationen SI1 von dem ersten Betriebssystem 16 einem in dem ersten Signalkonvertierungsmittel 15 aufgenommenen Modulator zugeführt, wobei der Modulator zur Durchführung einer Belastungsmodulation des Trägersignals gemäß den ersten Sendeinformationen SI1 ausgebildet ist.

Der Datenträger 1 weist weiters Speichermittel 17 zum Speichern von Daten auf. Solche Daten könne beispielsweise Geldbeträge, Beförderungseinheiten oder persönliche Daten eines Benutzers repräsentieren.

Das erste Betriebssystem 16 ist durch einen Mikroprozessor und ein in einem ROM gespeichertes und mit dem Mikroprozessor abarbeitbares erstes Programm gebildet, wie dies allgemein bekannt ist. Das erste Betriebssystems 16 bildet hierbei ein zwischen dem ersten Interface 10 und den Speichermitteln 17 aufgenommenes erstes Speicherzugriffsmittel 18 zum Zugreifen auf die Speichermittel 17.

Mit Hilfe des ersten Speicherzugriffsmittels 18 ist ein Zugreifen auf Daten ermöglicht, die in den Speichermitteln 17 der elektrischen Schaltung 12 gespeichert sind. Bei einem Zugreifen auf in den Speichermitteln 17 gespeicherte Daten ist ein Schreiben von Daten und ein Lesen von Daten durchführbar. Abgesehen von dem Zugreifen sind mit Hilfe eines in dem ersten Speicherzugriffsmittel 18 aufgenommen ersten Datenverarbeitungsmittels 19 das vorerwähnte erste Kommunikationsprotokoll und Rechenoperationen abarbeitbar. Gemäß dem ersten Kommunikationsprotokoll ist ein Authentisieren bei dem Zugreifen auf den ersten Speicherbereich 22 vorgesehen, wobei bei dem Authentisieren die Rechenoperationen angewendet werden, worauf nachfolgend noch eingegangen ist.

Der Datenträger 1 weist weiters Zugriffsermöglichungsmittel auf. Diese

Zugriffsermöglichungsmittel werden bei einem Zugreifen des ersten Speicherzugriffsmittels 18 auf die Speichermittel 17 durch eine Zugriffszuordnungsstufe 21 gemeinsam mit dem ersten Datenverarbeitungsmittel 19 gebildet. In der Zugriffsermöglichungsstufe 21, die durch ein ROM gebildet ist, sind zu allen adressierbaren Zugriffsadressen ZA der Speichermittel 17 korrespondierende Zugriffsermöglichungen ZE unveränderbar gespeichert. So zeigt beispielsweise eine logische Eins als die korrespondierende Zugriffsermöglichung ZE(n) zu der Zugriffsadresse ZA(n), daß ein Zugreifen des ersten Speicherzugriffsmittels 18 auf die Zugriffsadresse ZA(n) ermöglicht ist, wohingegen eine logische Nullen als die korrespondierende Zugriffsermöglichung ZE(m) zu der Zugriffsadresse ZA(m) anzeigt, daß ein Zugreifen des ersten Speicherzugriffsmittels (18) auf die Zugriffsadresse ZA(m) nicht ermöglicht ist.

Mit Hilfe der Zugriffsermöglichungsmittel ist bei dem Datenträger 1 eine erste Gliederung der Speichermittel 17 in einen ersten Speicherbereich 22 und einen zweiten Speicherbereich 23 und einen dritten Speicherbereich 24 realisiert, wobei mit Hilfe der in der Zugriffsermöglichungsstufe 21 gespeicherten Zugriffsermöglichungen ZE alleinig dem ersten Speicherzugriffsmittel 18 ein Zugreifen auf den ersten Speicherbereich 22 ermöglicht ist. Mit Hilfe der Zugriffsermöglichungen ZE ist dem ersten Speicherzugriffsmittel 18 auch ein Zugreifen auf den dritten Speicherbereich 24 ermöglicht, auf den auch noch ein zweites Speicherzugriffsmittel zugreifen kann, worauf hier aber nicht näher eingegangen ist.

Der Datenträger 1 weist weiters eine zweite Gliederung des ersten Speicherbereiches 22 in Sektoren auf. Jeder Sektor setzt sich aus vier Blöcken zusammen, wobei jeder Block sechzehn Byte umfaßt. In jedem Sektor ist ein Sektortrailer vorhanden, der durch den vierten Block gebildet ist. In dem Sektortrailer ist ein erster Schlüssel und ein zweiter Schlüssel gespeichert. Die Schlüssel dienen als Grundlage für das Authentisieren bei einem Zugreifen auf den ersten Speicherbereich 22.

Bei dem Authentisieren gemäß dem ersten Kommunikationsprotokoll wird sowohl in der ersten Kommunikationseinrichtung 2 eine erste Zufallszahl, die in der ersten Kommunikationseinrichtung 2 während des Authentisierens erhalten bleibt, als auch in dem ersten Datenverarbeitungsmittel 19 eine zweite Zufallszahl, die in dem ersten Datenverarbeitungsmittel 19 während des Authentisierens erhalten bleibt, generiert. Diese beiden Zufallszahlen werden zwischen dem Datenträger 1 und der ersten Kommunikationseinrichtung 2 kommuniziert und einerseits in der ersten

Kommunikationseinrichtung 2 die zweite Zufallszahl mit einem dritten Schlüssel verschlüsselt und andererseits von dem ersten Datenverarbeitungsmittel 19 die erste Zufallszahl mit dem ersten Schlüssel eines mit der Zugriffsadresse ZA adressierten Sektors verschlüsselt. Die beiden verschlüsselten Zufallszahlen werden zwischen dem Datenträger 1 und der ersten Kommunikationseinrichtung 2 kommuniziert. In der ersten Kommunikationseinrichtung 2 wird die verschlüsselte erste Zufallszahl mit Hilfe des dritten Schlüssels entschlüsselt, wodurch eine erste entschlüsselte Zufallszahl berechnet wird. In dem ersten Datenverarbeitungsmittel 19 wird die verschlüsselte zweite Zufallszahl mit Hilfe des ersten Schlüssels entschlüsselt, wodurch zweite entschlüsselte Zufallszahl berechnet wird. Das Authentisieren für das Zugreifen auf die Daten in dem mit Hilfe der Zugriffsadresse ZA adressierten Sektor ist dann erfolgreich abgeschlossen, wenn in der ersten Kommunikationseinrichtung 2 die erste erhalten gebliebene Zufallszahl mit der ersten entschlüsselten Zufallszahl übereinstimmt und wenn in dem ersten Datenverarbeitungsmittel 19 die zweite erhalten gebliebene Zufallszahl mit der zweiten entschlüsselten Zufallszahl übereinstimmt. Dies setzt voraus, daß der erste Schlüssel und der dritte Schlüssel identisch sind, oder anders formuliert, daß der ersten Kommunikationsstation 2 der Schlüssel des mit der Zugriffsadresse ZA adressierten Sektors bekannt sein muß.

Zusätzlich zu den beiden Schlüsseln sind in dem Sektortrailer noch eine Sektorzugriffsbedingung gespeichert, mit deren Hilfe für jeden Sektor das Zugreifen steuerbar ist. Darunter ist zu verstehen, daß auf die Daten eines ersten Sektors alleinig bei einem Schreiben von Daten zugreifbar ist, während auf einen zweiten Sektor alleinig bei einem Lesen von Daten zugreifbar ist. Weiters kann bei einem dritten Sektor sowohl ein Lesen von Daten als auch ein Schreiben von Daten durchführbar sein. Letztendlich kann bei einem vierten Sektor sowohl ein Schreiben als auch ein Lesen von Daten verboten sein, was beispielsweise für Daten zur Anwendung kommt, die ausschließlich bei einem Abarbeiten des ersten Betriebssystems 16 verwendet werden und demgemäß vor einem Zugreifen bei einer Kommunikation geschützt sein sollen.

Der Datenträger 1 weist weiters ein kontaktbehaftetes zweites Interface 25 zum Kommunizieren mit der zweiten Kommunikationseinrichtung 3 auf. In dem zweiten Interface 25 ist ein Kontaktfeld 26 des Kontaktepaares 9 aufgenommen, dessen Kontaktflächen mit den Kontakten der Kontaktmittel 8 in Kontaktverbindung bringbar sind. Eine erste Gruppe von Anschlüssen des Kontaktfeldes 26 ist mit einem Schaltungsteil des zweiten Interfaces 25, nämlich mit einem in der elektrischen Schaltung 12 enthaltenen

zweiten Versorgungsspannungsmittel 27 verbunden. Eine zweite Gruppe von Anschlüssen des Kontaktfeldes 26 ist mit einem weiteren Schaltungsteil des zweiten Interfaces 25, nämlich mit einem in der elektrischen Schaltung 12 enthaltenen zweiten Taktgenerator 28 verbunden. Eine dritte Gruppe von Anschlüssen des Kontaktfeldes 26 ist mit einem weiteren Schaltungsteil des zweiten Interfaces 25, nämlich mit einem in der elektrischen Schaltung 12 enthaltenen zweiten Signalkonvertierungsmittel 29 verbunden, wie dies gemäß dem Standard ISO7816 vorgesehen ist.

Dem zweiten Versorgungsspannungsmittel 27 kann über die erste Gruppe von Anschlüssen eine Spannung zugeführt werden. Aus dieser Spannung generiert das zweite Versorgungsspannungsmittel 27 eine zweiten Versorgungsspannung V2, die für eine elektrische Versorgung der elektrischen Schaltung 12 bei einer kontaktbehafteten Kommunikation vorgesehen ist. Bei einem Auftreten eines nominalen Wertes der zweiten Versorgungsspannung V2 wird von dem zweiten Versorgungsspannungsmittel 27 ein zweites Startsignal POR2 an ein zweites Betriebssystem 30 abgegeben.

Der zweite Taktgenerator 28 kann über die zweite Gruppe von Anschlüssen mit einem Taktsignal gespeist werden und generiert bei einer Speisung einen zweiten Systemtakt CLK2. Der zweite Systemtakt CLK2 wird dem zweiten Betriebssystem 30 als Betriebstakt zum Zweck eines synchronen Bearbeitens von zwischen dem zweiten Signalkonvertierungsmittel 29 und dem zweiten Betriebssystem 30 bidirektional austauschbaren zweiten Empfangsinformationen EI2 und zweiten Sendeinformationen SI2 zugeführt.

Das zweite Signalkonvertierungsmittel 29 wird über die dritte Gruppe von Anschlüssen gespeist und führt eine Pegelanpassung der zweiten Empfangsinformation EI2 und der zweiten Sendeinformationen SI2 bei einer Kommunikation über das zweite Interface 25 durch.

Das zweite Betriebssystem 30 ist durch den Mikroprozessor und ein in dem ROM gespeichertes und mit dem Mikroprozessor abarbeitbares zweites Programm gebildet, wobei von dem zweiten Betriebssystem 30 ein zweites Datenverarbeitungsmittel 31 und ein Schnittstellenmittel 32 in der Figur 1 dargestellt sind. Mit Hilfe des zweiten Datenverarbeitungsmittels 31 ist ein zweites Kommunikationsprotokoll abarbeitbar. Gemäß dem zweiten Kommunikationsprotokoll ist ein Authentisieren bei einem Zugreifen auf den zweiten Speicherbereich vorgesehen, wobei auf das Authentisieren bei dem Zugreifen auf den zweiten Speicherbereich nicht näher eingegangen wird. Weiters ist gemäß dem zweiten Kommunikationsprotokoll ein verschlüsseltes kontaktbehaftetes

Kommunizieren vorgesehen, so daß die von dem zweiten Signalkonvertierungsmittel 29 abgegebenen zweiten Empfangsinformationen EI2 von dem zweiten Datenverarbeitungsmittel 31 zunächst entschlüsselt werden und nachfolgend dem Schnittstellenmittel 32 zugeführt werden.

Der Datenträger 1 weist weiters zwischen dem zweiten Interface 25 und den Speichermitteln 17 ein zweites Speicherzugriffsmittel 33 zum Zugreifen auf die Speichermittel 17 auf. Hierbei enthält das zweite Speicherzugriffsmittel 33 das Schnittstellenmittel 32, welches einen Zugriffsanfragepuffer 34, einen Statusempfangspuffer 35 und einen Zugriffsdatenpuffer 36 beinhaltet.

Mit Hilfe des Zugriffsanfragepuffers 34 werden bei einem Zugreifen des zweiten Speicherzugriffsmittels 33 auf die Speichermittel 17 Zugriffsparameter ZP von dem zweiten Betriebssystem 30 an das ersten Betriebssystem 16 übermittelt und von dem zweiten Speicherzugriffsmittel 33 bearbeitet. Die zu übermittelnden Zugriffsparameter ZP sind beispielsweise eine Zugriffsadresse ZA, ein erster Zugriffscode ZC1 und eine erste Zugriffsbedingung ZB1. Unter einem ersten Zugriffscode ZC1 kann beispielsweise ein Paßwort verstanden werden. Eine erste Zugriffsbedingung ZB1 kann beispielsweise kennzeichnen , daß ein Schreiben von Daten in die Speichermittel 17 oder ein Lesen von Daten aus den Speichermitteln 17 angefragt ist.

Mit Hilfe des Statusempfangspuffers 35 ist von dem ersten Betriebssystem 16 ein Zugriffsstatus ZS an das zweite Betriebssystem 30 und hierbei an das zweite Datenverarbeitungsmittel 31 übermittelbar, wobei der Zugriffsstatus ZS in einem ersten Status ein erfolgreiches Zugreifen oder in einem zweiten Status ein erfolgloses Zugreifen auf die Speichermittel 17 anzeigt.

Bei angezeigtem ersten Status kann ein Zugreifen über den Zugriffsdatenpuffer 36 auf mit der Zugriffsadresse ZA adressierte Daten erfolgen, worauf nachfolgend anhand eines ersten Anwendungsbeispiels noch näher eingegangen ist. Bei angezeigtem zweiten Status muß ein Abbrechen des Zugreifens auf die Speichermittel 17 von dem zweiten Betriebssystem 30 durchgeführt werden.

Gemäß dem zweiten Kommunikationsprotokoll wird auch der Zugriffsstatus ZS und werden gegebenenfalls auch die von dem Zugriffsdatenpuffer 36 her zu dem zweiten Datenverarbeitungsmittel 31 zuführbaren Daten von dem zweiten Datenverarbeitungsmittel 31 zunächst verschlüsselt und als zweite Sendeinformationen SI2 an das zweite Signalkonvertierungsmittel 29 abgegeben.

Das zweite Speicherzugriffsmittel 33 weist ein Zugriffsfreigabemittel 37 auf, das bei

einem Zugreifen des zweiten Speicherzugriffsmittels 33 auf die Speichermittel 17 zusammen mit der Zugriffsermöglichungsstufe 21 Zugriffsermöglichungsmittel bildet. Mit Hilfe des Zugriffsfreigabemittels 37 kann von dem zweiten Speicherzugriffsmittel 33 aufgrund einer über den Zugriffsanfragepuffer 34 zugeführten Zugriffsadresse ZA eine Zugriffsermöglichung ZE überprüft werden. Bei einem Vorliegen einer Zugriffsermöglichung ZE wird von dem Zugriffsfreigabemittel 37 auf durch die Zugriffsadresse ZA adressierte Daten des zweiten Speicherbereiches 23 oder des dritten Speicherbereiches 24 der Speichermittel 17 ein Zugreifen durchgeführt. Bei dem Zugreifen werden Daten entweder zwischen dem zweiten Speicherbereich 23 oder zwischen dem dritten Speicherbereich 24 und dem Zugriffsdatenpuffer 36 über das Zugriffsfreigabemittel 37 ausgetauscht. Mit dem Zugriffsfreigabemittel 37 wird weiters der Zugriffsstatus ZS über den Statusempfangspuffer 35 dem zweiten Datenverarbeitungsmittel 31 des zweiten Betriebssystems 30 zugeführt.

Aufgrund der in der Zugriffsermöglichungsstufe 21 einander zugeordnet gespeicherten Zugriffsadressen ZA und Zugriffsermöglichungen ZE ist bei einem Zugreifen des zweiten Speicherzugriffsmittels 33 auf die Speichermittel 17 dem zweiten Speicherzugriffsmittel 33 ein alleiniges Zugreifen auf den zweiten Speicherbereich 23 und ein Zugreifen auf den dritten Speicherbereich 24 ermöglicht.

Im Folgenden ist nunmehr anhand eines ersten Anwendungsbeispiels für den Datenträger 1 gemäß dem Ausführungsbeispiel der Erfindung gemäß Figur 1 die Arbeitsweise der Smart-Card, also des erfindungsgemäßen Datenträgers 1, erläutert. Gemäß diesem ersten Anwendungsbeispiel ist angenommen, daß der Datenträgers 1 von einem ersten Systembetreiber, nämlich von einem Bankunternehmen als elektronische Geldbörse zur Verfügung gestellt wird.

Hierbei sind bei einem Bankterminal nach einer Identifikation eines Benutzers Geldbeträge in Form von Gelddaten GD bei einem Zugreifen auf den zweiten Speicherbereich 23 des Datenträgers 1 aufbuchbar oder abbuchbar. Ein Aufbuchen und ein Abbuchen der Geldbeträge erfolgt bei einer kontaktbehafteten Kommunikation zwischen einem Bankterminal, das mit der zweiten Kommunikationseinrichtung 3 zum kontaktbehafteten Kommunizieren ausgerüstet ist, und dem kontaktbehafteten zweiten Interface 25 des Datenträgers 1. Gemäß dem ersten Anwendungsbeispiel ist angenommen, daß der Benutzer des Datenträgers 1 einhundert Schilling von seinem Konto bei dem Bankunternehmen in die elektronische Geldbörse aufbuchen möchte, wofür den einhundert Schilling entsprechende aufzubuchende Gelddaten GD in die Speichermittel 17 gespeichert

werden sollen. Hierfür steckt der Benutzer die Smart Card in einen Schlitz des Bankterminals, worauf eine kontaktbehaftete Kommunikation beginnt.

Im Ablauf einer hierauf beginnenden Kommunikation zwischen dem zweiten Interface 25 und dem zweiten Sende/Empfangsmittel 7 der zweiten Kommunikationseinrichtung 3 werden aufzubuchende und einhundert Schilling repräsentierende zweite Sendedaten SD2 an das zweite Signalkonvertierungsmittel 25 kommuniziert. Das zweite Signalkonvertierungsmittel 25 erzeugt aus den zweiten Sendedaten SD2 zweite Empfangsinformationen EI2, deren Inhalt sich gemäß dem ersten Anwendungsbeispiel auf das Aufbuchen von einhundert Schilling entsprechenden Gelddaten GD in die Daten des zweiten Speicherbereiches 23 der Speichermittel 17 bezieht. Der Inhalt besteht hierbei aus den Zugriffsparametern ZP, die eine Zugriffsadresse ZA, nämlich die Zugriffsadresse ZA der elektronischen Geldbörse, eine erste Zugriffsbedingung ZB1, nämlich eine einem Aufbuchen entsprechende erste Zugriffsbedingung ZB1, und die den einhundert Schilling entsprechenden und aufzubuchenden Gelddaten GD aufweisen.

Die zweiten Empfangsinformationen EI2 werden von dem zweiten Datenverabeitungsmittel 31 aufgenommen und entschlüsselt. Die Zugriffsparameter ZP werden an den Zugriffsanfragepuffer 34 übergeben.

Gemäß der Zugriffsadresse ZA ermittelt das erste Zugriffsfreigabemittel 37 des zweiten Speicherzugriffsmittels 33, ob für die zugeführte Zugriffsadresse ZA in dem zweiten Speicherbereich 23 eine Zugriffsermöglichung ZE zum Lesen und zum Schreiben für mit der Zugriffsadresse ZA adressierte Gelddaten GD der Speichermittel 17 vorliegt. Bei einem Vorliegen dieser Zugriffsermöglichung ZE wird von dem ersten Zugriffsfreigabemittel 37 zunächst ein Zugreifen auf die in dem zweiten Speicherbereich 23 unter der Zugriffsadresse ZA gespeicherten alten Gelddaten GD in dem Sinne durchgeführt, daß die alten Gelddaten GD gelesen werden. Gemäß dem ersten Anwendungsbeispiel sollen diese alten Gelddaten GD einem Betrag von zwanzig Schilling entsprechen. Die alten Gelddaten werden von dem ersten Zugriffsfreigabemittel 37 über den Zugriffsdatenpuffer 36 an das zweite Datenverarbeitungsmittel 31 übergeben, wo die alten Gelddaten GD zu den aufzubuchenden Gelddaten GD addiert werden Damit ergeben sich einhundertundzwanzig Schilling repräsentierende neu Gelddaten GD, die von dem zweiten Datenverarbeitungsmittel 31 über den Zugriffsdatenpuffer 36 an das erste Zugriffsfreigabemittel 37 übergeben werden. Die neuen Gelddaten GD werden von dem ersten Zugriffsfreigabemittel 37 bei dem Zugreifen in Form des Schreibens als Daten in dem zweiten Speicherbereich 23 auf der Zugriffsadresse ZA gespeichert. Mit diesem

Zugreifen ist das Aufbuchen von einhundert Schilling entsprechenden und aufzubuchenden Gelddaten GD abgeschlossen und der Zugriffsstatus ZS wird dem zweiten Datenverarbeitungsmittel 31 von dem zweiten Speicherzugriffsmittel 33 über den Statusempfangspuffer 35 mitgeteilt und in weiter Folge an die zweite Kommunikationseinrichtung 3 in Form der zweiten Empfangsdaten ED2 kommuniziert, wo das erfolgreiche Aufbuchen dem Benutzer des Datenträgers 1 mitgeteilt wird und die Kommunikation beendet wird.

In Analogie zu dem im vorhergehenden Absatz beschriebenen Aufbuchen von aufzubuchenden Gelddaten GD erfolgt das Abbuchen von abzubuchenden Gelddaten GD beispielsweise bei einer Kassa, die zum kontaktbehafteten Kommunizieren mit dem Datenträger 1 ausgebildet ist, wobei im Ablauf einer Kommunikation lediglich von den alten Gelddaten GD die einem Wert einer zu bezahlenden Rechnung entsprechenden und abzubuchenden Gelddaten GD subtrahiert werden und die so erhaltenden neuen Gelddaten GD gespeichert werden.

Im Folgenden ist nunmehr anhand eines zweiten Anwendungsbeispiels für den Datenträger 1 gemäß dem Ausführungsbeispiel der Erfindung gemäß Figur 1 die Arbeitsweise der Smart-Card, also des erfindungsgemäßen Datenträgers 1, erläutert. Gemäß dem zweiten Anwendungsbeispiel ist angenommen, daß der Datenträger 1 von einem zweiten Systembetreiber, nämlich einem öffentlichen Beförderungsunternehmen, als elektronischer Fahrschein zur Verfügung gestellt wird.

Hierbei werden bei einem Aufbuchungsterminal gegen eine Bezahlung von Beförderungsgebühren Beförderungseinheiten entsprechenden Beförderungsdaten BD bei einem Zugreifen auf den ersten Speicherbereich 22 des Datenträgers 1 aufgebucht. Ein Aufbuchen von Beförderungseinheiten erfolgt bei einer kontaktlosen Kommunikation zwischen dem Aufbuchungsterminal, die mit der ersten Kommunikationseinrichtung 2 zum kontaktlosen Kommunizieren ausgerüstet ist, und dem kontaktlosen ersten Interface 10 des Datenträgers 1. Ein Abbuchen von Beförderungseinheiten erfolgt bei einer kontaktlosen Kommunikation zwischen einem Zugangsterminal zu Beförderungsmitteln des Beförderungsunternehmens, wobei das Zugangsterminal ebenfalls mit der ersten Kommunikationseinrichtung 2 zum kontaktlosen Kommunizieren ausgerüstet ist. Gemäß dem zweiten Anwendungsbeispiel ist angenommen, daß ein Benutzer fünf (5) Beförderungseinheiten auf den elektronischen Fahrschein aufbuchen möchte, wofür den fünf (5) Beförderungseinheiten entsprechende und aufzubuchende Beförderungsdaten BD in den Speichermitteln 17 gespeichert werden sollen.

Zum Zweck des Aufbuchens von Beförderungseinheiten wird der Datenträger 1 in den Kommunikationsbereich des Aufbuchungsterminals eingebracht. Gemäß dem ersten Kommunikationsprotokoll erfolgt nach dem Start des ersten Betriebssystems eine Selektion des Datenträgers 1. Bei einem selektierten Datenträger 1 wird in weiterer Folge im Zuge einer Kommunikation das Aufbuchen der Beförderungsdaten BD in den ersten Speicherbereich 22 durchgeführt.

Im Ablauf einer Kommunikation zwischen dem ersten Interface 10 und der ersten Kommunikationseinrichtung 2 werden den aufzubuchenden fünf (5) Beförderungseinheiten entsprechende erste Sendedaten SD1 an das erste Signalkonvertierungsmittel 15 kommuniziert. Das erste Signalkonvertierungsmittel 15 erzeugt aus den ersten Sendedaten SD1 erste Empfangsinformationen EI1, deren Inhalt sich gemäß dem zweiten Anwendungsbeispiel auf das Aufbuchen der den fünf (5) Beförderungseinheiten entsprechenden und aufzubuchenden Beförderungsdaten BD in die Daten des ersten Speicherbereiches 22 der Speichermittel 17 bezieht. Die ersten Empfangsinformationen EI1 werden zunächst von dem ersten Datenverarbeitungsmittel 19 gemäß dem ersten Kommunikationsprotokoll entschlüsselt.

Aufgrund einer in den Inhalten der ersten Empfangsinformationen EI1 enthaltenen Zugriffsadresse ZA ermittelt nun das gemeinsam mit der Zugriffsermöglichungsstufe 21 Zugriffsermöglichungsmittel bildende erste Datenverarbeitungsmittel 19, ob für die Zugriffsadresse ZA eine Zugriffsermöglichung ZE zum Zugreifen auf den ersten Speicherbereich 22 vorliegt.

Bei dem Vorliegen einer Zugriffsermöglichung ZE und bei dem nachfolgend erfolgreich abgeschlossenen Authentisieren ist von dem ersten Speicherzugriffsmittel 18 aus auf die in den Sektoren des ersten Speicherbereichs 22 gespeicherten Beförderungsdaten BD zugreifbar.

Bei einem Vorliegen einer Zugriffsermöglichung ZE wird von dem ersten Datenverarbeitungsmittel 19 zunächst ein Zugreifen auf die in dem ersten Speicherbereich 22 unter der Zugriffsadresse ZA gespeicherten alten Beförderungsdaten BD in dem Sinne durchgeführt, daß die alten Beförderungsdaten BD gelesen werden. Gemäß dem zweiten Anwendungsbeispiel sollen diese alten Beförderungsdaten BD drei (3) Beförderungseinheiten repräsentieren. Das erste Datenverarbeitungsmittel 19 addiert daraufhin zu den alten Beförderungsdaten BD die fünf (5) Beförderungseinheiten entsprechenden und aufzubuchenden Beförderungsdaten BD. Damit ergeben sich acht (8) Beförderungseinheiten entsprechende neue Beförderungsdaten BD, die von dem ersten

Datenverarbeitungsmittel 19 bei dem Zugreifen in Form des Schreibens als Beförderungsdaten in dem ersten Speicherbereich 23 auf der Zugriffsadresse ZA gespeichert werden. Mit diesem Zugreifen ist das Aufbuchen von fünf (5) Beförderungseinheiten repräsentierenden und aufzubuchenden Beförderungsdaten BD abgeschlossen. Das abgeschlossene Aufbuchen wird in Form der ersten Empfangsdaten ED1 an die kontaktlose erste Kommunikationseinrichtung 2 des Aufbuchungsterminals kommuniziert, wo das erfolgreiche Aufbuchen dem Benutzer des Datenträgers 1 mitgeteilt wird und die Kommunikation beendet wird.

In Analogie zu dem vorstehend beschriebenen Aufbuchen von aufzubuchenden Beförderungsdaten BD erfolgt das Abbuchen von abzubuchenden Beförderungsdaten BD, wobei im Ablauf einer Kommunikation von dem ersten Datenverarbeitungsmittel 19 lediglich von den alten Beförderungsdaten BD die abzubuchenden Beförderungsdaten BD subtrahiert werden und die so erhaltenen neuen Beförderungsdaten BD gespeichert werden.

Im Folgenden ist nunmehr anhand eines dritten Anwendungsbeispiels des Datenträgers 1 gemäß dem Ausführungsbeispiel der Erfindung gemäß der Figur 1 die Arbeitsweise der Smart-Card, also des erfindungsgemäße Datenträger 1, erläutert. Gemäß diesem dritten Anwendungsbeispiel ist nunmehr angenommen, daß das Bankunternehmen und das Beförderungsunternehmen kooperieren und daß bei einem Bankterminal, also einem Aufbuchungsterminal, Beförderungseinheiten in den ersten Speicherbereich 22 aufbuchbar sein sollen.

Hierfür weist der Datenträger 1 nunmehr erfindungsgemäß vorgesehene Speicherzusatzzugriffsmittel 38 auf.

Die Speicherzusatzzugriffsmittel 38 sind zum Zusammenwirken mit den zweiten Speicherzugriffsmitteln 33 und zum Zugreifen auf den ersten Speicherbereich 22 vorgesehen und zum Prüfen von einer Zugriffsberechtigung ausgebildet, so daß nach einem positiven Ergebnis der Prüfung der Zugriffsberechtigung zusätzlich von dem zweiten Speicherzugriffsmittel 33 her über die Speicherzusatzzugriffsmittel 38 und über das erste Speicherzugriffsmittel 18 auf den ersten Speicherbereich 22 zugreifbar ist.

Hierdurch ist der Vorteil erhalten, daß bei einer kontaktbehafteten Kommunikation mit einem Bankterminal über das zweite Interface 25 von dem zweiten Betriebssystem 30 nach dem Prüfen einer Zugriffsberechtigung und dem Erhalt eines positiven Ergebnisses der Prüfung dieser Zugriffsberechtigung über das erste Betriebssystem 16 auf den ersten Speicherbereich 22 zugreifbar ist. Damit ist bei der Kooperation für beide Systembetreiber

eine hohe Sicherheit gegenüber unbefugte Zugriffe auf ihre Speicherbereiche gewährleistet.

Ein weiterer Vorteil ist durch das Vorsehen einer Prüfung einer Zugriffsberechtigung dahingehend erhalten, daß dies eine flexible Gestaltung wie auch eine flexible Verwaltung dieser Zugriffsberechtigung ermöglicht. So kann beispielsweise bei einer unsachgemäßen Verwendung des Datenträgers 1 auf einfachste Weise bei einer kontaktlosen Kommunikation mit einem Zugangsterminal des Beförderungsunternehmens jegliche weitere Verwendung des Datenträgers als elektronischer Fahrschein im Zusammenhang mit den erfindungsgemäßen Maßnahmen unterbunden werden, obwohl der Datenträger 1 als elektronische Geldbörse uneingeschränkt weiter verwendet werden kann. Weiters ist der Vorteil erhalten, daß eine Nutzung von bereits in dem ersten Betriebssystem implementierten Softwareroutinen ermöglicht ist, wodurch sich die erfindungsgemäßen Merkmale auf besonders einfache Weise realisieren lasen.

Die Speicherzusatzzugriffsmittel 38 sind in den ersten Speicherzugriffsmitteln 18 aufgenommen und weisen ein zweites Zugriffsfreigabemittel 39 auf, das aufgrund einer zuführbaren Zugriffsadresse ZA zusammen mit der Zugriffsermöglichungsstufe 21 Zugriffsermöglichungsmittel bildet, die zum Ermitteln einer Zugriffsermöglichung ZE auf die Speichermittel 17 vorgesehen sind.

Hierdurch ist der Vorteil erhalten, daß ein mit Hilfe der Zugriffsermöglichungsmittel realisiertes Unterbinden eines direkten Zugreifens von dem zweiten Betriebssystem 30 auf den ersten Speicherbereich 22 aufrecht erhalten bleibt. Durch das Vorliegen einer Zugriffsermöglichung für ein Zugreifen von dem in dem ersten Betriebssystem 16 aufgenommenen Speicherzusatzzugriffsmittel 38 ist jedoch ein Zugreifen von dem zweiten Betriebssystem 30 über das Speicherzusatzzugriffsmittel 38 auf den ersten Speicherbereich 22 ermöglicht. Weiters ist durch das Unterbinden eines direkten Zugreifens von dem zweiten Betriebsystem 30 auf den ersten Speicherbereich 22 sichergestellt, daß das Zugreifen auf die Beförderungsdaten mit einwandfreier Konsistenz erfolgt, weil das Zugreifen nur mit einem Teil des ersten Betriebssystems 16 – nämlich dem Speicherzusatzzugriffsmittel 38 - ermöglicht ist. Damit ist ein unsachgemäßes Zugreifen wie beispielsweise ein fehlerhaftes Schreiben von Beförderungsdaten durch das zweite Betriebssystem 30 des Bankunternehmens in den ersten Speicherbereich 22 ausgeschlossen.

Die Speicherzusatzzugriffsmittel 38 weisen weiters Zugriffscodeprüfmittel 40 zum Prüfen von einem Zugriffscode auf. Das Zugriffscodeprüfmittel 40 ist symbolisch als

UND-Gatter dargestellt, von welchem ein erstes Prüfergebnis B1 an ein Prüfergebnisverknüpfungsmittel 41, das ebenfalls als UND-Gatter symbolisiert ist, abgebbar ist. Das erste Prüfergebnis B1 wird auch über den Statusempfangspuffer 35 dem zweiten Betriebssystem 30 verfügbar gemacht. Den Zugriffscodeprüfmitteln 40 ist einerseits ein erster Zugriffscode ZC1 von dem zweiten Speicherzugriffsmittel 33 her über den Zugriffsanfragepuffer 34 zuführbar und andererseits ein zweiter Zugriffscode ZC2 zuführbar, der mit dem ersten Schlüssel und dem zweiten Schlüssel berechenbar ist, die in dem ersten Speicherbereich 22 gespeichert sind. Das Übereinstimmen des ersten Zugriffscodes ZC1 und des zweiten Zugriffscodes ZC2 ist Voraussetzung für das Positive Ergebnis der Prüfung der Zugriffsberechtigung.

Hierbei ist der Vorteil erhalten, daß für den Ursprung des zuführbaren Zugriffscodes ZC1 eine größtmögliche Flexibilität herrscht. So kann vorteilhafter Weise der zuführbare Zugriffscode ZC1 bei einer Kommunikation zwischen dem Datenträger 1 und einer kontaktbehafteten Kommunikationseinrichtung 3 kommuniziert werden, was besonders dann Sinn ergibt, wenn jedem Benutzer ein zuführbarer Zugriffscode ZC1 verfügbar sein soll. Es kann aber auch eine Speicherung des zuführbaren Zugriffscode ZC1 in dem zweiten Speicherbereich 23 von Vorteil sein, wenn von dem Benutzer nicht bei jedem Aufbuchen von Beförderungseinheiten eine Neueingabe des zuführbaren Zugriffscodes ZC1 über das Bankterminal verlangt wird. Weiters kann auch bei extremen Anforderungen an eine Geheimhaltung des zuführbaren Zugriffscodes ZC1 eine Berechnung des zuführbaren Zugriffscodes ZC1 mit Hilfe der zweiten Datenverarbeitungsmittel 31 aus Daten, die bei einer Kommunikation übertragen werden, oder aus Daten, die in den Speichermitteln 17 gespeichert sind, von Vorteil sein.

In dem Speicherzusatzzugriffsmittel 38 ist weiters zum Berechnen des berechenbaren zweiten Zugriffscodes ZC2 ein Zugriffscodeberechnungsmittel 41 vorgesehen, das zum Abarbeiten eines Triple DES Verschlüsselungsverfahrens gemäß dem Standard ISO/IEC 10116 ausgebildet ist. Im Fall des Vorliegens einer Zugriffsermöglichung ZE für eine Zugriffsadresse ZA wird von dem zweiten Zugriffsfreigabemittel 39 ein Zugreifen auf einen mit Hilfe der Zugriffsadresse ZA adressierten Sektor des ersten Speicherbereichs 22 durchgeführt, bei dem ein Lesen des ersten Schlüssels und des zweiten Schlüssels erfolgt. Mit Hilfe des zweite Zugriffsfreigabemittels 39 wird dem Zugriffscodeberechnungsmittel 42 der erste Schlüssel und der zweite Schlüssel zugeführt und somit das Berechnen des zweiten Zugriffscodes ZC2 ermöglicht und von dem Zugriffscodeberechnungsmittel 42 durchgeführt. Hierbei sei erwähnt, daß das Triple DES Verschlüsselungsverfahren den

ersten Schlüssel und den zweiten Schlüssel zur Berechnung des zweiten Zugriffscodes ZC2 benötigt.

Hierdurch ist der Vorteil erhalten, daß die für die Grundlage des Authentisierens gemäß dem ersten Kommunikationsprotokoll bei dem Zugreifen auf die Sektoren des ersten Speicherbereiches verwendeten Schlüssel weiterhin geheim gehalten werden können und dem Bankunternehmen lediglich der aus den Schlüsseln berechenbare Zugriffscode ZC1 bekannt sein muß.

Hierdurch weiters ist der Vorteil erhalten, daß die Berechnung des zweiten Zugriffscodes ZC2 wesentlich beschleunigt ist, weil das Zugriffscodeberechnungsmittel 42 vorteilhafter Weise als Krypto-Co-Prozessor ausgebildet ist.

Ein weiterer Vorteil ist dadurch erhalten, daß durch die Abarbeitung des Triple DES Verschlüsselungsverfahrens eine Rückrechnung auf die Schlüssel unterbunden ist.

Die Speicherzusatzzugriffsmittel 38 weisen zusätzlich zu den Zugriffscodeprüfmitteln 40 Zugriffsbedingungsprüfmittel 43 zum Prüfen von einer Zugriffsbedingung auf. Das Zugriffsbedingungsprüfmittel 43 ist symbolisch als UND-Gatter dargestellt, von welchem ein zweites Prüfergebnis B2 an das Prüfergebnisverknüpfungsmittel 41 abgebbar ist. Den Zugriffsbedingungsprüfmitteln 43 ist einerseits eine erste Zugriffsbedingung ZB1 von dem zweiten Speicherzugriffsmittel 33 über den Zugriffsanfragepuffer 34 her zuführbar und andererseits ist eine zweite Zugriffsbedingung ZB2 zuführbar, die als die Sektorzugriffsbedingung aus den Daten ermittelbar ist, die in dem ersten Speicherbereich 22 gespeichert sind. Im Fall des Vorliegens einer Zugriffsermöglichung ZE für eine Zugriffsadresse ZA wird von dem zweiten Zugriffsfreigabemittel 39 ein Zugreifen auf Daten eines mit Hilfe der Zugriffsadresse ZA adressierten Sektors des ersten Speicherbereiches 22 durchgeführt, wobei diese Daten die Sektorzugriffsberechtigung repräsentieren. Die Sektorzugriffsberechtigung wird von dem zweiten Zugriffsfreigabemittel 39 gelesen und dem Zugriffsbedingungsprüfmittel 43 als die zweite Zugriffsbedingung ZB2 zugeführt.

Hierdurch ist der Vorteil erhalten, daß zum Schutz gegenüber unbefugten Zugriffen auf den ersten Speicherbereich 22 bei der Prüfung von Zugriffsberechtigungen zusätzlich zu der Prüfung des Zugriffscodes ZC1 eine Prüfung der Zugriffsbedingung ZB1 vorgesehen ist. Somit kann selbst bei einem Übereinstimmen eines zuführbaren Zugriffscodes mit einem berechenbaren Zugriffscode eine zusätzliche Prüfung erfolgen, bevor endgültig bei einer zusätzlichen Übereinstimmung dieser Zugriffsbedingungen ein positives Ergebnis der Prüfung der Zugriffsberechtigung vorliegt. Durch diese Maßnahme ist eine hierarchische

Vergabe der Zugriffsberechtigung vorsehbar. Es kann beispielsweise bei einer Kommunikation des Datenträgers 1 mit der kontaktlosen Kommunikationseinrichtung 2 eines Zugangsterminals des Beförderungsunternehmens ein Problem bei dem Abbuchen von Beförderungseinheiten auftreten, das nicht vor Ort gelöst werden kann. Dieses Problem kann beispielsweise eine gravierende Überschreitung der auf dem Datenträger gespeicherten Beförderungseinheiten sein. Von dem Zugangsterminal kann nun während der Kommunikation eine Zugriffsbedingung für die Beförderungseinheiten entsprechenden Beförderungsdaten BD derart geändert werden, daß bei einem Bankterminal selbst bei einer Eingabe eines gültigen Zugriffscodes kein Aufbuchen von Beförderungseinheiten mehr möglich ist. Bei der Kommunikation mit dem Bankterminal kann dem Benutzer dann eine Nachricht angezeigt werden, in der er aufgefordert wird, ein Aufbuchungsterminal aufzusuchen, um das aufgetretene Problem zu lösen. Bei einem aufgetretenen Problem bei einer sachgemäßen Benutzung des Datenträgers 1 ist also mit Hilfe der hierarchischen Vergabe der Zugriffsberechtigung eine Neuvergabe des Zugriffscodes ZC1 nicht zwingend erforderlich. Bei dem Aufbuchungsterminal kann dem Benutzer das aufgetretene Problem erklärt werden und gegebenenfalls die Zugriffsbedingung für die Beförderungseinheiten entsprechenden Beförderungsdaten BD derart geändert werden, daß bei einem Bankterminal wieder das Aufbuchen von Beförderungseinheiten entsprechenden Beförderungsdaten BD möglich ist.

Das Übereinstimmen einerseits des ersten Zugriffscodes ZC1 und des zweiten Zugriffscodes ZC2, repräsentiert durch das erste Prüfergebnis B1, und andererseits das Übereinstimmen der ersten Zugriffsbedingung ZB1 und der zweiten Zugriffsbedingung ZB2, repräsentiert durch das zweite Prüfergebnis B2, ist eine Voraussetzung für das Positive Ergebnis der Prüfung der Zugriffsberechtigung. Das Ergebnis der Prüfung der Zugriffsberechtigung wird mit Hilfe des Prüfergebnisverknüpfungsmittel 41, das als ein UND Gatter symbolisiert ist, generiert und als drittes Prüfergebnis B3 einerseits an das zweite Zugriffsfreigabemittel 39 und andererseits an den Statusempfangspuffer 35 weitergeleitet.

Gemäß dem dritten Anwendungsbeispiel ist angenommen, daß der Benutzer des Datenträgers 1 ein Abbuchen von einhundert Schilling bei einem Bankterminal von seinem Konto durchführt und gleichzeitig an dem Bankterminal das Aufbuchen der einhundert Schilling als Beförderungseinheiten in dem ersten Speicherbereich 22 des Datenträgers 1 durchführt, in welchem ersten Speicherbereich 22 Beförderungseinheiten entsprechende alte Beförderungsdaten BD des Beförderungsunternehmens gespeichert sind. Hierzu steckt

der Benutzer die Smart Card in einen Schlitz des Bankterminals, worauf eine kontaktbehaftete Kommunikation über das Kontaktepaar 9 beginnt. Der Benutzer identifiziert sich zunächst als legitimierter Benutzer für das zweite Betriebssystem des Bankunternehmens. Mit Hilfe eines Eingabefeldes äußert er seinen Wunsch, Beförderungseinheiten in die Speichermittel 17 des Datenträgers 1 aufzubuchen und diese Beförderungseinheiten direkt über sein Konto bei dem Bankunternehmen zu bezahlen. Er wird aufgefordert den Betrag, den er in Beförderungseinheiten investieren möchte, in das Bankterminal einzugeben. Danach wird er aufgefordert, den ersten Zugriffscode ZC1 einzugeben, mit dem er sich als legitimierter Benutzer für das zweite Betriebssystem des Beförderungsunternehmens identifiziert.

Bei einer hierauf beginnenden Kommunikation zwischen dem zweiten Interface 25 und dem zweiten Sende/Empfangsmittel 7 der zweiten Kommunikationseinrichtung 3 können nun auch gemäß dem dritten Anwendungsbeispiel zweite Empfangsinformationen EI2 auftreten, deren Inhalt sich auf das Aufbuchen der Beförderungseinheiten entsprechenden aufzubuchenden Beförderungsdaten BD in den ersten Speicherbereich 22 bezieht. Die zweiten Empfangsinformationen EI2 werden von dem zweiten Betriebssystem 30 aufgenommen und von dem zweiten Datenverarbeitungsmittel 31 dem Schnittstellenmittel 32 zugeführt, wo eine Abgabe der Zugriffsparameter ZP über das zweite Speicherzugriffsmittel 33 an das Speicherzusatzzugriffsmittel 38 erfolgt. Weiters wird über den Zugriffsanfragepuffer 34 der erste Zugriffscode ZC1 an die Zugriffscodeprüfmittel 40 und die erste Zugriffsbedingung ZB1 an das Zugriffsbedingungsprüfmittel 43 abgegeben.

Im Folgenden wird das Zugreifen auf den ersten Speicherbereich 22 der Speichermittel 17 des Datenträgers 1 mit Hilfe eines erfindungsgemäßen Verfahrens 44 beschrieben, das durch das in der Figur 2 dargestellte Flußdiagramm 44 repräsentiert ist.

Bei einem Block 45 beginnt die Abarbeitung des erfindungsgemäßen Verfahrens 44, wenn die Zugriffsparameter ZP an den Zugriffsanfragepuffer 34 abgegeben werden.

Bei einem nachfolgenden Block 46 ermitteln die aus dem zweiten Zugriffsfreigabemittel 39 und der Zugriffsermöglichungsstufe 21 gebildeten Zugriffsermöglichungsmittel aufgrund der Zugriffsadresse ZA zunächst, ob eine Zugriffsermöglichung ZE für eine Zugriffsadresse ZA des ersten Speicherbereichs 22 vorliegt.

Im Fall einer fehlenden Zugriffsermöglichung ZE wird bei einem Block 47 dem zweiten Betriebssystem 30 über den Stauempfangspuffer 34 der Zugriffsstatus ZS mitgeteilt, daß das Zugreifen nicht ermöglicht ist. Daraufhin kommuniziert das zweite

Betriebssystem 30 den Zugriffsstatus ZS an die zweite Kommunikationseinrichtung 3 und das Speicherzusatzzugriffsmittel 38 bricht das Zugreifen auf den ersten Speicherbereich 22 ab, worauf das erfindungsgemäße Verfahren 44 bei dem Block 48 beendet wird.

Im Fall einer vorliegenden Zugriffsermöglichung ZE wird bei einem Block 49 zunächst der berechenbare zweite Zugriffscode ZC2 von dem Zugriffscodeberechnungsmittel 42 berechnet.

Bei einem Block 50 wird anschließend der berechenbare zweite Zugriffscode ZC2 mit dem zuführbaren ersten Zugriffscode ZC1 mit Hilfe des Zugriffscodeprüfmittels 40 verglichen. Aufgrund des so erhaltenen ersten Prüfergebnisses B1 wird entschieden, ob das Zugreifen fortgesetzt wird oder ob das Zugreifen abgebrochen wird.

Im Fall eines Fehlens einer Übereinstimmung des ersten Zugriffscodes ZC1 mit dem zweiten Zugriffscode ZC2 wird das Verfahren 44 bei dem Block 47 fortgesetzt und bei dem Block 48 beendet.

Im Fall eines Übereinstimmens des ersten Zugriffscodes ZC1 mit dem zweiten Zugriffscode ZC2 wird das Verfahren 44 bei einem Block 51 fortgesetzt, bei dem die erste Zugriffsbedingung ZB1 und die zweite Zugriffsbedingung ZB2 verglichen werden und ein zweites Prüfergebnis B2 erhalten wird. Aufgrund des so erhaltenen zweiten Prüfergebnisses B2 wird entschieden, ob das Zugreifen fortgesetzt wird oder ob das Zugreifen abgebrochen wird.

Im Fall eines Fehlens einer Übereinstimmung der ersten Zugriffsbedingung ZB1 mit der zweiten Zugriffsbedingung ZB2 wird das Verfahren 44 bei dem Block 47 fortgesetzt und bei dem Block 48 beendet. Im Fall eines Übereinstimmens der ersten Zugriffsbedingung ZB1 mit der zweiten Zugriffsbedingung ZB2 wird das Verfahren 44 bei einem Block 52 fortgesetzt, bei dem das Zugreifen auf den ersten Speicherbereich 22 durchgeführt wird und anschließend das Zugreifen bei dem Block 48 beendet wird.

Bei diesem Zugreifen auf den ersten Speicherbereich 22 erfolgt zunächst mit Hilfe des zweiten Zugriffsfreigabemittels 39 ein Lesen der alten Beförderungsdaten BD und ein Übergeben der alten Beförderungsdaten BD über den Zugriffsdatenpuffer 36 an das zweite Datenverabeitungsmittel 31, wo die alten Beförderungsdaten BD zu den aufzubuchenden Beförderungsdaten BD addiert werden. Die so erhaltenen neuen Beförderungsdaten BD werden über den Zugriffsdatenpuffer 36 an das zweite Zugriffsfreigabemittel 39 übergeben und von dem Zugriffsfreigabemittel 39 bei einem Zugreifen in Form des Schreibens als Daten in dem ersten Speicherbereich 22 auf der Zugriffsadresse ZA gespeichert. Damit sind wie von dem Benutzer verlangt, die einhundert Schilling entsprechenden

Beförderungseinheiten als aufzubuchende Beförderungsdaten BD in den ersten Speicherbereich 22 des Beförderungsunternehmens aufgebucht.

Gemäß dem dritten Anwendungsbeispiel muß also der zweiten Kommunikationseinrichtung 3 des zweiten Systembetreibers lediglich ein aus zwei Schlüsseln eines Sektors des ersten Speicherbereiches 22 mit Hilfe eines Triple DES Verfahrens berechenbarer erster Zugriffscode ZC1 bekannt sein, der mit dem zweiten Zugriffscode ZC2 identisch ist. Im vorliegenden Fall wurde der erste Zugriffscode ZC1 der zweiten Kommunikationseinrichtung 3 bei einer Eingabe des ersten Zugriffscodes ZC1 über das Bankterminal verfügbar gemacht. Daher ist mit Hilfe des erfindungsgemäßen Speicherzusatzzugriffsmittels 38 erreicht, daß bei einer Kommunikation über das kontaktbehaftete zweite Interface 25 des Datenträgers 1 ein Zugreifen auf den ersten Speicherbereich 22 ermöglicht ist, obwohl alleinig dem ersten Systembetreiber die Schlüssel der Sektoren des ersten Speicherbereiches 22 bekannt sind. Dadurch ist ein von dem ersten Systembetreiber geforderter Schutz der in dem ersten Speicherbereich 22 gespeicherten Daten vor einem unbefugten Zugreifen bei einer Kooperation der beiden Systembetreiber gewährleistet. Zusätzlich zu diesem Schutz ergibt sich für den Benutzer des Datenträgers 1 der Vorteil, daß er das Aufbuchen von Beförderungseinheiten direkt bei einem Bankterminal vollziehen kann und er sich dadurch zusätzliche Wegzeiten erspart.

Es kann erwähnt werden, daß bei einem Zugreifen auf die Speichermittel 17 die gemeinsam mit der Zugriffsermöglichungsstufe 21 Zugriffsermöglichungsmittel bildenden Mittel 19, 37, 39 auf eine gemeinsame Softwareroutine zugreifen können, die ein Bestandteil des ersten Betriebssystems 16 ist.

Es kann erwähnt werden, daß die Zugriffsermöglichungsmittel und das erfindungsgemäß vorgesehene Speicherzusatzzugriffsmittel 38 Bestandteile eines Master-Betriebssystems sind, das einem oder mehreren anderen Betriebssystemen übergeordnet ist, und daß nur mit Hilfe dieser zwei Bestandteile ein Zugreifen auf die Speichermittel 17 möglich ist.

Es kann erwähnt werden, daß der erfindungsgemäße Datenträger 1 als Bestandteil eines Schlüssels oder eines Schlüsselanhängers ausgebildet sein kann. Weiters kann der erfindungsgemäße Datenträger 1 ein Bestandteil eines Schmuckstückes, wie etwa einer Uhr oder eines Ringes sein. Auch die Ausbildung eines erfindungsgemäßen Datenträgers 1 als Bestandteil eines Schreibutensils, wie etwa eines Kugelschreibers, sei erwähnt.

Es sei erwähnt, daß bei einem bekannten Datenträger 1 ein Interface-Umschaltmittel aufgenommen sein kann. Das Interface-Umschaltmittel dient zum Umschalten zwischen

dem ersten Interface 10 bei einer kontaktlosen Kommunikation mit einer kontaktlosen Kommunikationseinrichtung 2 und dem zweiten Interface 25 bei einer kontaktbehafteten Kommunikation mit einer kontaktbehafteten Kommunikationseinrichtung 3 bei dem Abarbeiten des zweiten Betriebssystems 30. Mit Hilfe des Interface-Umschaltmittels ist sowohl bei einer Kommunikation über das erste Interface 10 als auch bei einer Kommunikation über das zweite Interface 25 ein Zugreifen mit dem zweiten Betriebssystem 30 über das erste Betriebssystem 16 auf den ersten Speicherbereich 22 ermöglicht, wodurch beispielsweise das Bankunternehmen über Bankterminals sowohl zum kontaktlosen Kommunizieren wie auch zum kontaktbehafteten Kommunizieren verfügen kann. In diesem Zusammenhang ist auch zu erwähnen, daß das Interface-Umschaltmittel auch ein Abarbeiten des ersten Betriebssystems bei einem kontaktlosen Kommunizieren und auch bei einem kontaktbehafteten Kommunizieren ermöglichen kann.

Es kann erwähnt werden, daß ein Zugangsterminal durch ein mit einer kontaktlosen Kommunikationseinrichtung 2 ausgerüstetes Drehkreuz oder eine Zugangsschranke gebildet sein kann. Bei einem entsprechend weit reichenden Kommunikationsbereich der kontaktlosen Kommunikationseinrichtung 2 kann ein Bestandteil des Zugangsterminals auch durch einen Teil eines Teppichs oder einen Teil eines Fußbodens oder einen Teil einer Wandverkleidung oder Deckenverkleidung gebildet sein, in welchen Teil die Primärspule 5 der kontaktlosen Kommunikationseinrichtung 2 integriert ist. Unter einem Zugangsterminal kann auch eine mobile Entwerterstation, die über eine kontaktlose Kommunikationseinrichtung 2 verfügt und die beispielsweise von einem Schaffner getragen wird, verstanden werden.

Patentansprüche:

1. Datenträger (1) zum Speichern von Daten,
der ein erstes Interface (10) zum Kommunizieren mit einer ersten Kommunikationseinrichtung (2) aufweist und
der ein zweites Interface (25) zum Kommunizieren mit einer zweiten Kommunikationseinrichtung (3) aufweist und
der eine elektrische Schaltung (12) enthält,
die Schaltungsteile (13, 14, 15) von dem ersten Interface (10) und Schaltungsteile (27, 28, 29) von dem zweiten Interface (25) enthält und
die Speichermittel (17) zum Speichern von Daten aufweist, welche Speichermittel (17) einen ersten Speicherbereich (22) und einen zweiten Speicherbereich (23) aufweisen, und
die zwischen dem ersten Interface (10) und den Speichermitteln (17) ein erstes Speicherzugriffsmittel (18) zum Zugreifen auf die Speichermittel (17) aufweist und
die zwischen dem zweiten Interface (25) und den Speichermitteln (17) ein zweites Speicherzugriffsmittel (33) zum Zugreifen auf die Speichermittel (17) aufweist und
die Zugriffsermöglichungsmittel (21, 37, 39, 19) aufweisen, die alleinig dem ersten Speicherzugriffsmittel (18) ein Zugreifen auf den ersten Speicherbereich (22) ermöglichen,
dadurch gekennzeichnet,
daß der Datenträger (1) Speicherzusatzzugriffsmittel (38) aufweist, die zum Zusammenwirken mit den zweiten Speicherzugriffsmitteln (33) vorgesehen sind und die zum Zugreifen auf den ersten Speicherbereich (22) vorgesehen sind und die zum Prüfen von einer Zugriffsberechtigung für das Zugreifen auf den ersten Speicherbereich (22) ausgebildet sind, und
daß nach einem positiven Ergebnis der Prüfung der Zugriffsberechtigung zusätzlich von dem zweiten Speicherzugriffsmittel (33) her über die Speicherzusatzzugriffsmittel (38) und über das erste Speicherzugriffsmittel (18) auf den ersten Speicherbereich (22) zugreifbar ist.

2. Datenträger (1) nach Anspruch 1, dadurch gekennzeichnet,
daß die Speicherzusatzzugriffsmittel (38) in den ersten Speicherzugriffsmitteln (18) aufgenommen sind.

3. Datenträger (1) nach Anspruch 1, dadurch gekennzeichnet,
daß die Speicherzusatzzugriffsmittel (38) Zugriffscodeprüfmittel (40) zum Prüfen von einem Zugriffscode (ZC1) aufweisen und
daß den Zugriffscodeprüfmitteln (40) einerseits ein erster Zugriffscode (ZC1) von dem

zweiten Speicherzugriffsmittel (33) her zuführbar ist und andererseits ein zweiter Zugriffscode (ZC2) zuführbar ist, der aus Daten berechenbar ist, die in dem ersten Speicherbereich (22) gespeichert sind, und

daß das Übereinstimmen des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) Voraussetzung für das positive Ergebnis der Prüfung der Zugriffsberechtigung ist.

4. Datenträger (1) nach Anspruch 3, dadurch gekennzeichnet,

daß zum Berechnen des berechenbaren zweiten Zugriffscodes (ZC2) ein Zugriffscodeberechnungsmittel (42) vorgesehen ist und

daß das Zugriffscodeberechnungsmittel (42) zum Abarbeiten eines Triple DES Verschlüsselungsverfahrens ausgebildet ist.

5. Datenträger (1) nach Anspruch 3, dadurch gekennzeichnet,

daß die Speicherzusatzzugriffsmittel (38) zusätzlich zu den Zugriffscodeprüfmitteln (40) Zugriffsbedingungsprüfmittel (43) zum Prüfen von einer Zugriffsbedingung (ZB1) aufweisen und

daß den Zugriffsbedingungsprüfmitteln (43) einerseits eine erste Zugriffsbedingung (ZB1) von dem zweiten Speicherzugriffsmittel (33) her zuführbar ist und andererseits eine zweite Zugriffsbedingung (ZB2) zuführbar ist, die aus Daten ermittelbar ist, die in dem ersten Speicherbereich (22) gespeichert sind, und

daß das Übereinstimmen einerseits des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) und andererseits der ersten Zugriffsbedingung (ZB1) und der zweiten Zugriffsbedingung (ZB2) Voraussetzung für das positive Ergebnis der Prüfung der Zugriffsberechtigung ist.

6. Datenträger (1) nach Anspruch 1, dadurch gekennzeichnet,

daß die elektrische Schaltung (12) des Datenträgers (1) als integrierter Schaltkreis ausgebildet ist.

7. Elektrische Schaltung (12) für einen Datenträger (1) zum Speichern von Daten,

die Schaltungsteile (13, 14, 15) von einem ersten Interface (10) zum Kommunizieren mit einer ersten Kommunikationseinrichtung (2) enthält und

die Schaltungsteile (27, 28, 29) von einem zweiten Interface (25) zum Kommunizieren mit einer zweiten Kommunikationseinrichtung (3) enthält und

die Speichermittel (17) zum Speichern von Daten aufweist, welche Speichermittel (17) einen ersten Speicherbereich (22) und einen zweiten Speicherbereich (23) aufweisen, und

die zwischen den Schaltungsteilen (13, 14, 15) von dem ersten Interface (10) und den Speichermitteln (17) ein erstes Speicherzugriffsmittel (18) zum Zugreifen auf die

Speichermittel (22) aufweist und
die zwischen den Schaltungsteilen (27, 28, 29) von dem zweiten Interface (25) und den Speichermitteln (17) ein zweites Speicherzugriffsmittel (33) zum Zugreifen auf die Speichermittel (17) aufweist und
die Zugriffsermöglichungsmittel (21, 37, 39, 19) aufweisen, die alleinig dem ersten Speicherzugriffsmittel (18) ein Zugreifen auf den ersten Speicherbereich (22) ermöglichen, dadurch gekennzeichnet,
daß die Schaltung (12) Speicherzusatzzugriffsmittel (38) aufweist, die zum Zusammenwirken mit den zweiten Speicherzugriffsmitteln (33) vorgesehen sind und die zum Zugreifen auf den ersten Speicherbereich (22) vorgesehen sind und die zum Prüfen von einer Zugriffsberechtigung für das Zugreifen auf den ersten Speicherbereich (22) ausgebildet sind, und
daß nach einem positiven Ergebnis der Prüfung der Zugriffsberechtigung zusätzlich von dem zweiten Speicherzugriffsmittel (33) her über die Speicherzusatzzugriffsmittel (38) und über das erste Speicherzugriffsmittel (18) auf den ersten Speicherbereich (22) zugreifbar ist.

8. Schaltung (12) nach Anspruch 7, dadurch gekennzeichnet,
daß die Speicherzusatzzugriffsmittel (38) in den ersten Speicherzugriffsmitteln (18) aufgenommen sind.

9. Schaltung (12) nach Anspruch 7, dadurch gekennzeichnet,
daß die Speicherzusatzzugriffsmittel (38) Zugriffscodeprüfmittel (40) zum Prüfen von einem Zugriffscode (ZC1) aufweisen und
daß den Zugriffscodeprüfmitteln (40) einerseits ein erster Zugriffscode (ZC1) von dem zweiten Speicherzugriffsmittel (33) her zuführbar ist und andererseits ein zweiter Zugriffscode (ZC2) zuführbar ist, der aus Daten berechenbar ist, die in dem ersten Speicherbereich (22) gespeichert sind, und
daß das Übereinstimmen des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) Voraussetzung für das positive Ergebnis der Prüfung der Zugriffsberechtigung ist.

10. Schaltung (12) nach Anspruch 9, dadurch gekennzeichnet,
daß zum Berechnen des berechenbaren zweiten Zugriffscodes (ZC2) ein Zugriffscodeberechnungsmittel (42) vorgesehen ist und
daß das Zugriffscodeberechnungsmittel (42) zum Abarbeiten eines Triple DES Verschlüsselungsverfahrens ausgebildet ist.

11. Schaltung (12) nach Anspruch 9, dadurch gekennzeichnet,

daß die Speicherzusatzzugriffsmittel (38) zusätzlich zu den Zugriffscodeprüfmitteln (40) Zugriffsbedingungsprüfmittel (43) zum Prüfen von einer Zugriffsbedingung (ZB1) aufweisen und

daß den Zugriffsbedingungsprüfmitteln (43) einerseits eine erste Zugriffsbedingung (ZB1) von dem zweiten Speicherzugriffsmittel (33) her zuführbar ist und andererseits eine zweite Zugriffsbedingung (ZB2) zuführbar ist, die aus Daten ermittelbar ist, die in dem ersten Speicherbereich (22) gespeichert sind, und

daß das Übereinstimmen einerseits des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) und andererseits der ersten Zugriffsbedingung (ZB1) und der zweiten Zugriffsbedingung (ZB2) Voraussetzung für das positive Ergebnis der Prüfung der Zugriffsberechtigung ist.

12. Schaltung (12) nach Anspruch 7, dadurch gekennzeichnet,

daß die Schaltung (12) als integrierter Schaltkreis ausgebildet ist.

13. Verfahren (44) zum Zugreifen auf Speichermittel (17) eines Datenträgers (1) mit einem ersten Speicherbereich (22) und einem zweiten Speicherbereich (23), wobei das Verfahren (44) die nachfolgend angeführten Schritte enthält, nämlich

Speichern von Daten in zumindest dem ersten Speicherbereich (22) der Speichermittel (17),

Ermöglichen eines alleinigen Zugreifens von ersten Speicherzugriffsmitteln (18) auf den ersten Speicherbereich (22),

dadurch gekennzeichnet,

daß Speicherzusatzzugriffsmitteln (38) Zugriffsberechtigungen für das Zugreifen auf den ersten Speicherbereich (22) zugeführt werden und

daß die zugeführten Zugriffsberechtigungen mit Hilfe der Speicherzusatzzugriffsmittel (38) geprüft werden und

daß nach dem Prüfen der Zugriffsberechtigungen und bei einem Vorliegen eines positiven Ergebnisses der Prüfung zusätzlich von einem zweiten Speicherzugriffsmittel (33) her über die Speicherzusatzzugriffsmittel (38) und über das erste Speicherzugriffsmittel (18) auf den ersten Speicherbereich (22) zugegriffen wird.

14. Verfahren (44) nach Anspruch 13, dadurch gekennzeichnet,

daß bei dem Prüfen der Zugriffsberechtigungen mit Hilfe von Zugriffscodeprüfmitteln (40) ein erster Zugriffscode (ZC1) mit einem zweiten Zugriffscode (ZC2) verglichen wird und

daß der erste Zugriffscode (ZC1) von dem zweiten Speicherzugriffsmittel (33) her den Zugriffscodeprüfmitteln (40) zugeführt wird und

daß der zweite Zugriffscode (ZC2) aus Daten berechnet wird, die in dem ersten Speicherbereich (22) gespeichert sind, und
daß das Übereinstimmen des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) Voraussetzung für das positive Ergebnis der Prüfung bildet.

15. Verfahren (44) nach Anspruch 14, dadurch gekennzeichnet,
daß bei dem Prüfen der Zugriffsberechtigungen zusätzlich zu dem Vergleichen des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) mit Hilfe der Zugriffscodeprüfmittel (40) mit Hilfe von Zugriffsbedingungsprüfmitteln (43) eine erste Zugriffsbedingung (ZB1) mit einer zweiten Zugriffsbedingung (ZB2) verglichen wird und
daß die erste Zugriffsbedingung (ZB1) von dem zweiten Speicherzugriffsmittel (33) her den Zugriffsbedingungsprüfmitteln (43) zugeführt wird und die zweite Zugriffsbedingung (ZB1) aus Daten ermittelt wird, die in dem ersten Speicherbereich (22) gespeichert sind, und
daß das Übereinstimmen einerseits des ersten Zugriffscodes (ZC1) und des zweiten Zugriffscodes (ZC2) und andererseits der ersten Zugriffsbedingung (ZB1) und der zweiten Zugriffsbedingung (ZB2) Voraussetzung für das positive Ergebnis der Prüfung bildet.

Zusammenfassung

Datenträger zum Speichern von Daten und Schaltung für einen solchen Datenträger

Ein Datenträger (1), der zum Speichern von Daten in Speichermitteln (17) vorgesehen ist, weist ein erstes Speicherzugriffsmittel (18) zum Zugreifen auf einen ersten Speicherbereich (22) und ein zweites Speicherzugriffsmittel (33) zum Zugreifen auf einen zweiten Speicherbereich (23) auf, wobei auf den ersten Speicherbereich (22) mit Hilfe von Zugriffsermöglichungsmittel (21, 19, 37, 39) alleinig von dem ersten Speicherzugriffsmittel (18) zugreifbar ist, und weist weiters ein Speicherzusatzzugriffsmittel (38) auf, so daß bei einem Zugreifen von dem zweiten Speicherzugriffsmittel (33) bei einem Zusammenwirken mit dem zweiten Speicherzugriffsmittel (33) ein Prüfen einer Zugriffsberechtigung für das Zugreifen auf den ersten Speicherbereich (22) und ein Zugreifen auf den ersten Speicherbereich (22) durchführbar ist.

(Figur 1).

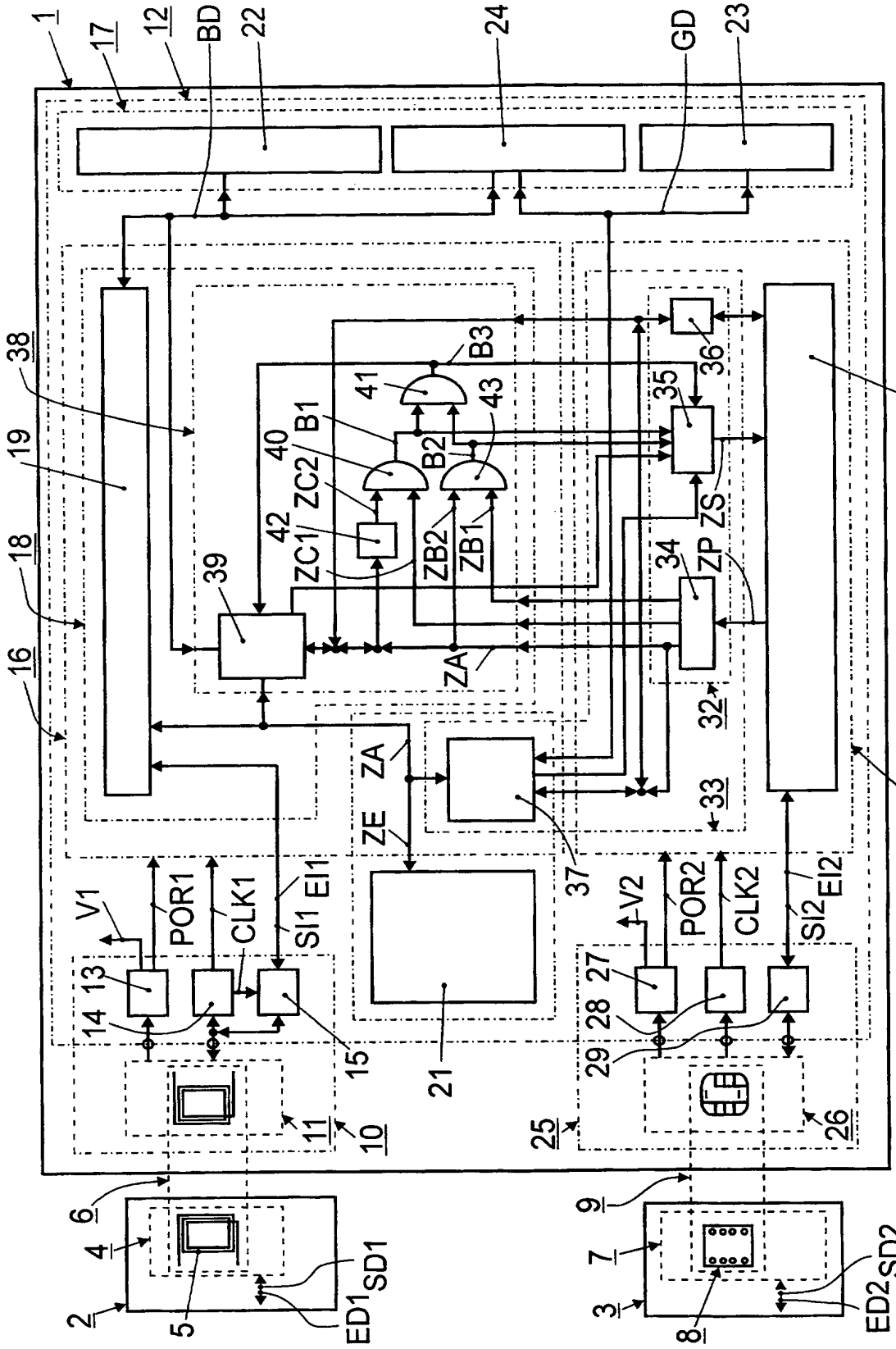

FIG. 1

1-II-PHO 99.534

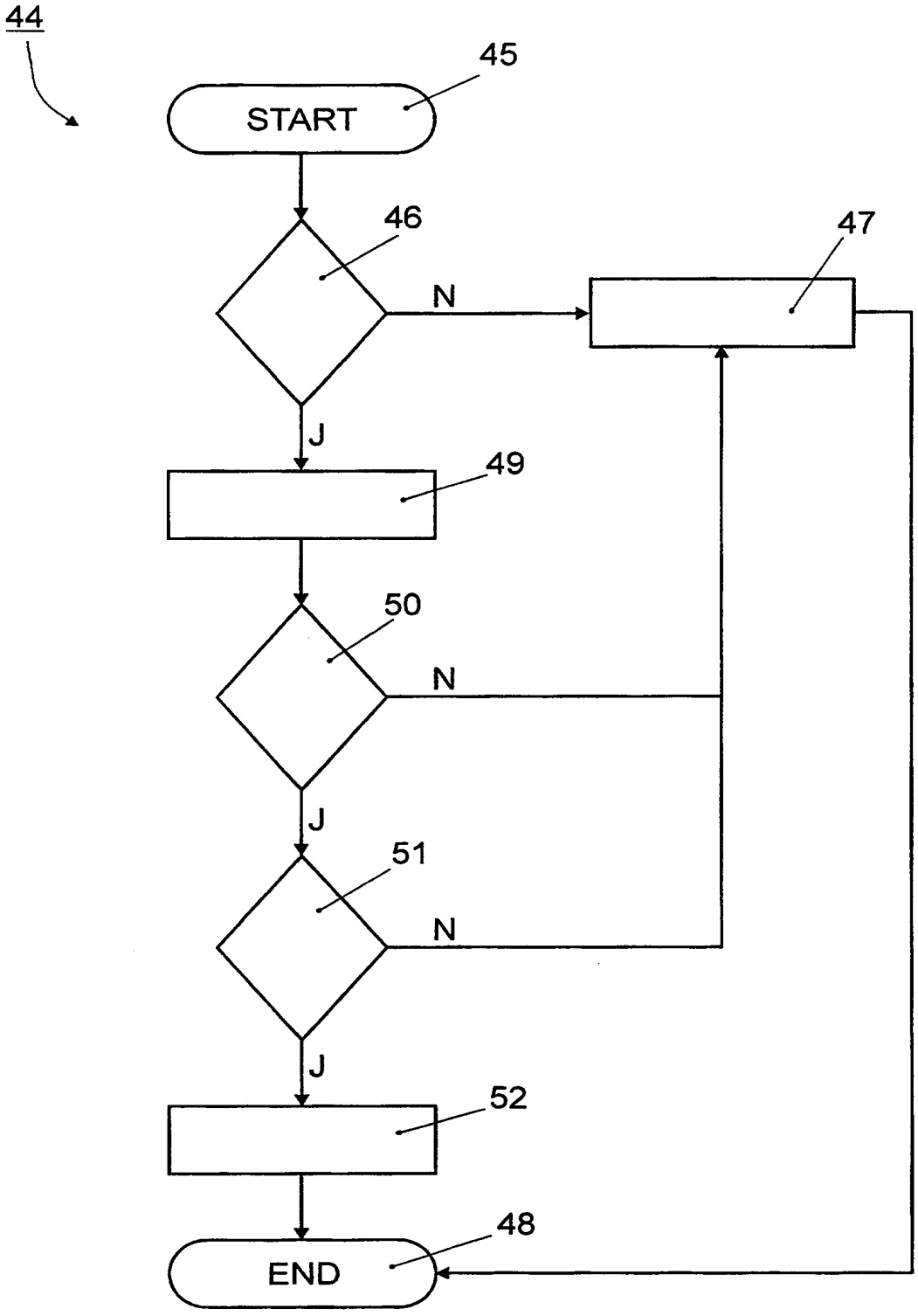

FIG. 2